Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of processing out-of-order messages, comprising:

determining, with a secure communication module of a client device, a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

comparing, with said secure communication module of said client device, a nonce value of a received out-of-order message with said largest nonce value yet seen;

comparing, with said secure communication module of said client device, said nonce value to nonce values within a single acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

adjusting, with said secure communication module of said client device, a size of a range of acceptable nonce values within said single acceptance window, where said size of said range is based on said determined largest nonce value yet seen; and

rejecting, with said secure communication module of said client device, said received out-of-order message if said nonce value falls outside said single acceptance window.

2. (previously presented) The method according to claim 1, further comprising:

designating, with said secure communication module of said client device, said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

3. (previously presented) The method according to claim 1, further comprising:

replacing, with said secure communication module of said client device, said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

4. (previously presented) The method according to claim 1, further comprising:

adjusting, with said secure communication module of said client device, said single acceptance window if said nonce value exceeds said largest nonce value yet seen.

5. (previously presented) The method according to claim 1, further comprising:

designating, with said secure communication module of said client device, said received out-of-order message as a replay attack.

6. (previously presented) The method according to claim 1, further comprising:

comparing, with said secure communication module of a client device, said nonce value to a window mask value if said nonce value falls within said single acceptance window; and

rejecting, with said secure communication module of a client device, said received out-of-order message if said nonce value is within said window mask value.

7. (previously presented) The method according to claim 6, further comprising:

designating, with said secure communication module of said client device, said received out-of-order message as part of a replay attack.

8. (previously presented) The method according to claim 1, further comprising:

comparing, with said secure communication module of said client device, said nonce value to a window mask value if said nonce value falls within said single acceptance window; and

accepting, with said secure communication module of said client device, said received out-of-order message if said nonce value is outside said window mask value.

9. (previously presented) The method according to claim 8, further comprising:

designating, with said secure communication module of a client device, said nonce value as a largest nonce value yet seen.

10. (currently amended) An apparatus for processing out-of-order messages, said apparatus comprising:

a communication interface configured to transmit and receive a plurality of packets; and

a controller, wherein said controller is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

compare a nonce value of a received out-of-order message and said largest nonce value yet seen;

compare said nonce value to nonce values within a single acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

adjust a size of a range of acceptable nonce values within said single acceptance window, where said size of said range is based on said determined largest nonce value yet seen; and

reject said received out-of-order message if said nonce value falls outside said single acceptance window.

11. (previously presented) The apparatus according to claim 10, wherein:

said controller is further configured to designate said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

12. (previously presented) The apparatus according to claim 10, wherein:

said controller is further configured to adjust said single acceptance window if said largest nonce value yet seen exceeds said largest nonce value yet seen.

13. (previously presented) The apparatus according to claim 10, wherein:

said controller is further configured to replace said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

14. (previously presented) The apparatus according to claim 10, wherein:

said controller is further configured to designate said received out-of-order message as part of a replay attack.

15. (previously presented) The apparatus according to claim 10, wherein said controller is further configured to:

compare said nonce value to a window mask value if said nonce value falls within said single acceptance window; and

reject said received out-of-order message if said nonce value falls outside said single acceptance window.

16. (previously presented) The apparatus according to claim 15, wherein:

said controller is further configured to designate said received out-of-order message as part of a replay attack.

17. (previously presented) The apparatus according to claim 10, wherein said controller is configured to:

compare said nonce value to an acceptance window value if said nonce value falls within said single acceptance window; and

accept said received out-of-order message if said nonce value falls within said single acceptance window.

18. (previously presented) The apparatus according to claim 17, wherein:

said controller is further configured to mark said nonce value as said largest nonce value yet seen.

19. (currently amended) A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of processing out-of-order messages, said one or more computer programs comprising a set of instructions for:

determining, with a secure communication module of a client device, a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

comparing, with said secure communication module of said client device, a nonce value of a received out-of-order message and said largest nonce value yet seen;

comparing, with said secure communication module of said client device, said nonce value to nonce values within a single acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

adjusting, with said secure communication module of said client device, a size of a range of acceptable nonce values within said single acceptance window, where said size of said range is based on said determined largest nonce value yet seen; and

rejecting, with said secure communication module of said client device, said received out-of-order message if said nonce value not falls within said single acceptance window.

20. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said client device, said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

21. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

replacing, with said secure communication module of said client device, said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

22. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

adjusting, with said secure communication module of said client device, said single acceptance window based on said nonce value if said nonce value exceeds said largest nonce value yet seen.

23. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said client device, said received out-of-order message as a replay attack.

24. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing, with said secure communication module of said client device, said nonce value to a window mask value if said nonce value falls within said single acceptance window; and

rejecting, with said secure communication module of said client device, said received out-of-order message if said nonce value falls outside said single acceptance window.

25. (previously presented) The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said client device, said received out-of-order message as part of a replay attack.

26. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing, with said secure communication module of said client device, said nonce value to a window mask value if said nonce value falls within said single acceptance window; and

accepting, with said secure communication module of said client device, said received out-of-order message if said nonce value falls within said single acceptance window.

27. (previously presented) The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said client device, said nonce value as said largest nonce value yet seen.

28. (currently amended) A system for processing out-of-order messages in a peer-to-peer configuration, comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a secure communication module configured to be executed by said first peer and second peer, wherein said secure communication module is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of a out-of-order messages;

compare a nonce value to a filter in response to said nonce value of a received out-of-order packet not exceeding said largest nonce value yet seen;

compare said nonce value to nonce values within a single replay mask;

adjust a size of a range of acceptable nonce values within said single replay mask, where said size of said range is based on said determined largest nonce value yet seen; and

accept said received out-of-order packet if said nonce value falls within said single replay mask.

29. (previously presented) The system according to claim 28, wherein:

said secure communication module is further configured to designate said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

30. (previously presented) The system according to claim 28, wherein:

said secure communication module is further configured to adjust said single replay mask based on said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

31. (previously presented) The system according to claim 28, wherein:

said secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside said single replay mask.

32. (previously presented) The system according to claim 31, wherein:

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

33. (previously presented) The system according to claim 32, wherein:

said secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside said single replay mask.

34. (previously presented) The system according to claim 33, wherein:

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

35. (previously presented) The system according to claim 28, wherein:

said secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside said single replay mask; and

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

36. (currently amended) An interceptor device for processing out-of-order messages, said interceptor device comprising:

a network interface;

an expected sequence register configured to enumerate an expected sequence number of a packet received out-of-order from a second network device;

a memory configured to store a single replay mask; and

a controller, wherein said controller is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

compare a nonce value to a filter in response to a sequence number of a received out-of-order packet via said network interface does not exceed said largest nonce value yet seen retrieved from said expected sequence register;

compare said sequence number to said single replay mask retrieved from said memory;

adjust a size of a range of acceptable nonce values within said single replay mask, where said size of said range is based on said determined largest nonce value yet seen; and

accept said received out-of-order packet if said sequence number falls within said single replay mask.

37. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to designate said sequence number as said largest nonce value yet seen if said sequence number exceeds said largest sequence number yet seen.

38. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to adjust said single replay mask based on said largest nonce value yet seen if said sequence number exceeds said largest nonce value yet seen.

39. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside said single replay mask.

40. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

41. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside said single replay mask.

42. (previously presented) The interceptor device according to claim 41, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

43. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside said single replay mask; and

said controller is further configured to designate said received out-of-order packet as part of a replay attack.